CHAPTER 8

A Runner's Mobile App

"I'm an instant star. Just add water."

—David Bowie

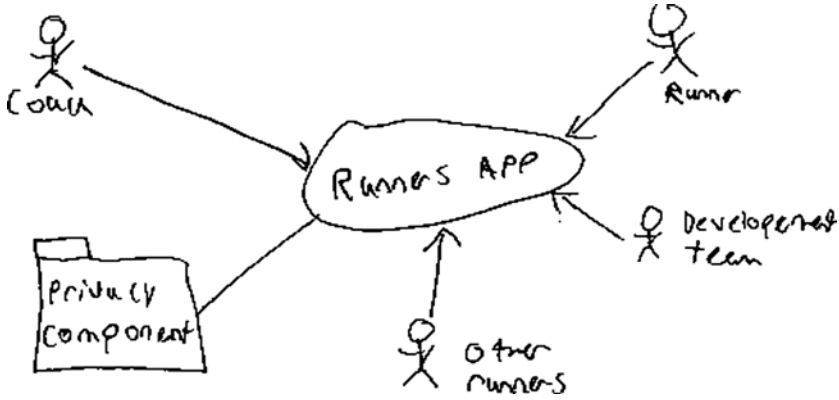
This chapter describes the process of designing a small mobile app using privacy engineering methodology. This example scenario shows how these methods can be used for small apps and systems. The runner's mobile app began, as discussed in the sidebar, as a discussion between grandfather and grandson concerning the usefulness of the privacy engineering methodology for designing an app.

MY GRANDSON, CODESLINGER AND PRIVACY ENGINEER IN THE MAKING

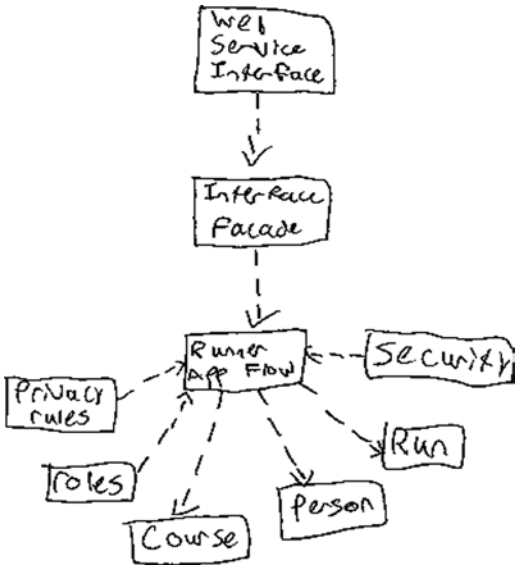
by Tom Finneran & R Traver Clifford

My grandson, Traver, was looking forward to his summer internship at the end of his junior year in high school with a company that builds apps for smartphones. I asked him if he knew how to design an app. He wasn't sure. So we sat down to discuss app design. He wanted a runner's app. We went through the who, what, where, when, how, and why as pertains to a runner's app using the requirements gathering for UML systems engineering lifecycle planning. The next step was to create a context diagram (shown below) showing potential users of the app, including the runner, the coach, and other runners as stakeholders. We then leveraged various UML diagrams and the other aspects of our methodology. His draft runner's app could be created and implemented with a data-centric, privacy engineered architecture. His component diagram is also shown below.

The modeling and planning processes are as appropriate for a single developer acting as a part-time summer worker for a large and complex global enterprise. Privacy engineering is not too cumbersome for the small or the cash strapped. No excuses and, in this case, gain with no pain.



Traver's context diagram



Traver's component diagram

The runner's mobile app could use a simple version of the privacy component, as will be discuss in this chapter. It will be used to track cross-country race results as well as practice runs. The original intent of the runner's app was use as a smartphone or tablet app. The runner's app could be a web application that uses a PC, a school server, or could run in the Cloud as well.

The development team, including a privacy team representative, will add a Privacy Notice and privacy rules tied to the roles, and a simplified privacy component can be invoked by the runner's app. The coach, runner, and other runner will be able to interact within the runner's app (Figure 8-1).

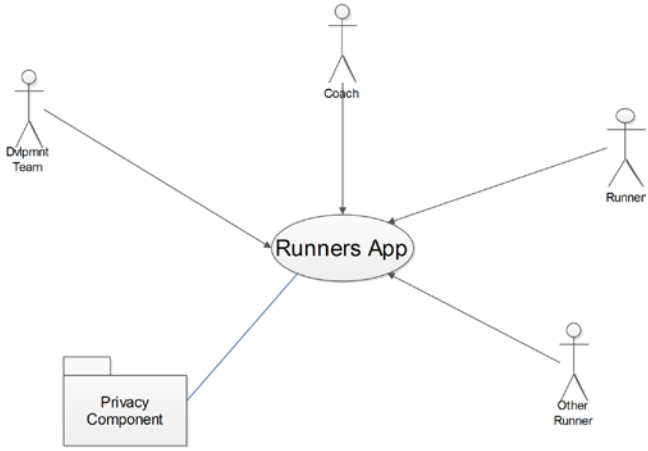


Figure 8-1. *Runner's app context diagram*

The Runner's Mobile App Use Case

The runner's mobile app design began with the development of a use case, as discussed in Chapters 5 and 6. One important requirement that needs to be considered within the runner's app is compliance with the requirements for collecting personal information from minors. Many countries have restrictions on collecting and using personal information from children and what is necessary to consider the processing fair and legitimate. For instance, in the United States, the Children's Online Privacy Protection Act (COPPA), among other things, requires verifiable parental consent before one can collect data from children under 13 years old. If your app will collect or process personal information from children, make sure you understand the associated requirements and use cases.[1]

These are the answers to the six use case questions, as outlined in Chapter 7:

- *Why*: Record a runner's runtime on a given cross-country course against an appropriate standard. The app will be used by the runners on a team and by their coaches.

[1]COPPA requires a Privacy Notice that describes the type of information collected, how parents can give permission, how information collected from the child will be used, whether it would be distributed to other third parties, and how the parents can contact the web site operator by phone or e-mail. The Federal Trade Commission provides a guide to COPPA on their web site.

- *Who*:
  - Individual person:
    - Runner role
    - Coach role
    - Other runner role
    - Development team
- *When*:
  - Application of data-related events:
    - Need to enter/maintain courses
    - Need to enter/maintain standard for courses
    - Need to enter/maintain runner information
    - Need to enter/maintain run
    - Need to present run history
    - Need to correct data
    - Need to enter/maintain archive rules, for all data, including privacy rules
  - Privacy-related events:
    - Privacy Notice needed
    - Need to enter and maintain privacy rules
    - Need to enter/maintain roles
    - Need to encrypt
- *How*:
  - Application related:
    - Maintain courses
    - Maintain course standards for each runner level
    - Enter runner information
    - Enter run on course
    - Present run history report
    - Run archiving rules

        - Privacy related:
            - Maintains a Privacy Notice
            - Which data are collected
            - Which roles and how date are used
            - Which rules, including children's privacy requirements, if needed
            - Who can see what
        - Maintain privacy rules for each role
        - Request notice
- *What*:
    - Privacy rule
    - Runner role
    - Other runner role
    - Coach role
    - Individual person
    - Course
    - Run
    - Run history
- *Where*:
    - Mobile:
        - Smartphone
        - Tablet
    - School server
    - Cloud

The Runner's App Class or Data Model

In developing the runner's app class or data model, take into account the team requirements and a simplified privacy component data model.

In Figure 8-2, the various *roles* may have one or more *privacy rules* related to them. The *runner role* is related to one *individual person* at a time, whereas the *other runner roles* and the *coach's role* may be related to more than one *person*. An *individual* may make multiple *runs* on multiple *courses*. The *run history* consists of information about multiple *runs*.

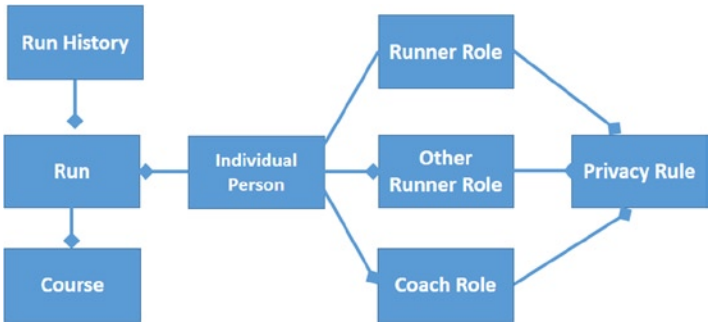


Figure 8-2. *Runner's app class or data model*

ADDITIONAL REQUIREMENT

After the fact, as a part of our book review process, an additional requirement surfaced. A *team* class should probably be included in the data model. This would enable the app to be used for more than one team at the same time. This is just one example of how as you progress within the methodology new requirements surface.

The Runner's App User Experience Requirements

The development team is supported by a privacy expert who develops a Privacy Notice that contains:

- Which data are collected
- Which roles the data benefit and how they are used
- Which rules are applied
- Who can see what

The development team and the privacy expert enter the privacy rules for each role. The coach enters information about each course, both practice courses and competitive courses. Course information contains course standards for rookie runners, junior runners, and senior runners as determined by the coach. The runner can enter his or her times and review runs and the run history against the appropriate course standard. The coach can review runs and the run history for all runners on his or her team and can correct any data-entry mistakes. Runners may be allowed to check other runners' times if those runners allow that. A runner can run the run history report for his or her runs and for other runners' runs when he or she has been granted permission. The coach can run archiving rules at the end of the season.

Design the App Structure

The runner's app will be structured according to the component metadata model discussed in Chapters 6 and 7. Thus, it will have a user interface that takes in data from both the app's database, designed from the data model, and from data entered by the various actors. It will have an event handler for events contained in the use case and behaviors listed in the "how" section of the use case.

The coach, the runner, and the other runners will be able to use the component user interface for adding data, correcting data, and requesting information. Run, course, and individual data will be drawn from the database that may be stored on the device, on the school server, or in the Cloud. Event handling and behavior execution may be done on the device, on the school web site server, or in the Cloud. The technical design team makes those platform decisions once the design is completed.

The Runner's App System Activity Diagram

The runner's app system activity diagram (Figure 8-3) shows the development team, consisting of the designer or developer and a privacy expert, utilizing an administrative module for setting up the app. All system users have to sign on regardless of their role. The runner adds the data into the data collection module. The runner, other runners, and the coach may all perform queries or run the history report as long as they are given permission. The coach will perform data correction in the data correction module and will work with the development team on handling archiving.

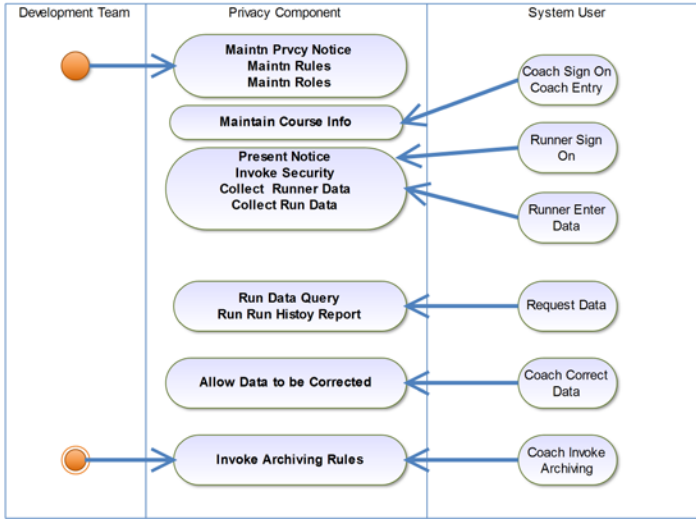


Figure 8-3. *Runner's app system activity diagram*

Privacy Assessment Using a System Activity Diagram

Figure 8-4 shows the privacy principles satisfied by the various runner's app modules.

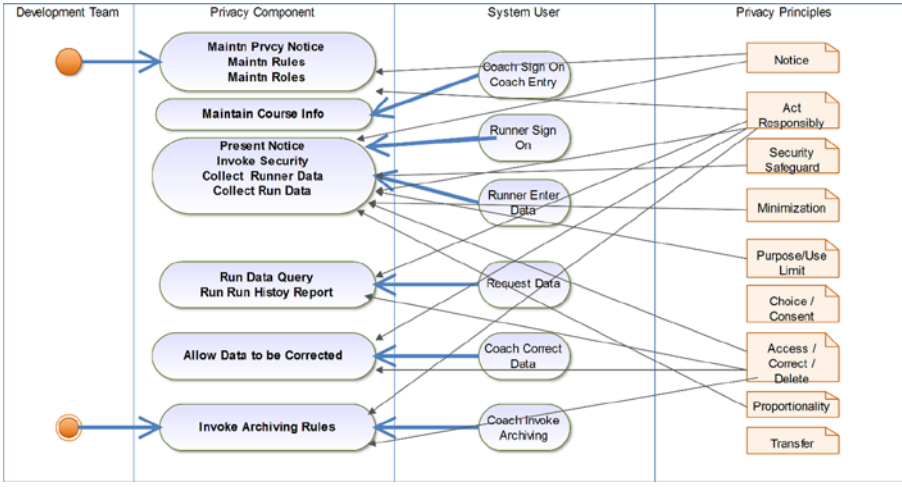


Figure 8-4. *Runner's app system activity privacy assessment*

Develop the Runner's App Component Design

Figure 8-5 shows the runner's app interface subcomponent, which may be implemented by means of a smartphone, tablet, or web site. The interface facade accepts the data from whichever source and presents it in a common format to the runner's app flow handler. We could simplify the design by deciding what the user interface source is and eliminate the interface facade pattern. This is a design decision. The runner's app flow handler controls the flow of the privacy rules subcomponent, the security subcomponent, the individual person subcomponent, the roles subcomponent, the course subcomponent, and the run subcomponent.

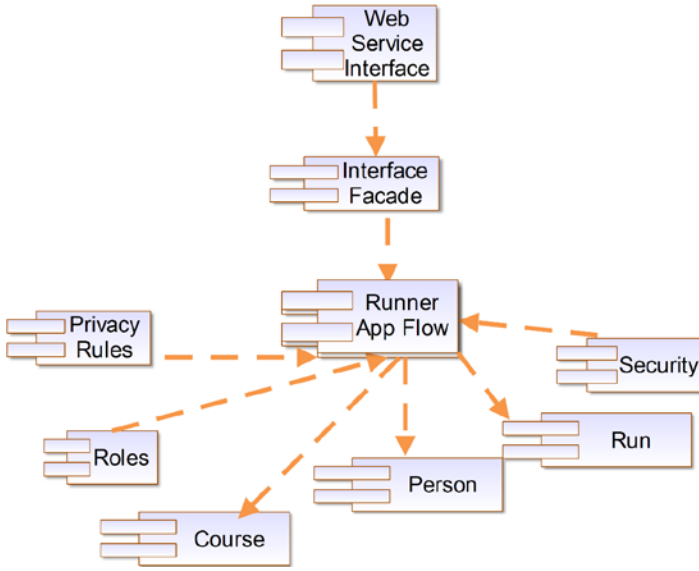


Figure 8-5. *Runner's app component diagram*

Using the System Development Methodology

For an application as simple as the runner's app, the steps described in Chapter 6 should be followed but in a less formal manner. Project management can be simpler, although there should be a simple project plan and project status measurements. In the case of the runner's app, our scoping workshop and the initial use case development was a 2-hour discussion. The modeling approach recommended in this book provides simple but extremely useful documentation that facilitates a correct, well-designed, maintainable application.

Conclusion

This chapter included the runner's app design because it was a fun, interesting incident that happened while in the process of writing this book—using its methodology to help a teenager understand how to design an app. More important, the app development process shows you how the privacy engineering methodology can be used for small individual applications as well as for large enterprise applications, as will be discussed in Chapter 9. A small application may not have a privacy component available or may not even need a privacy component. However, an app like this, especially where younger children may be involved, does require privacy protection. Any small app requires a disciplined design and development methodology with sufficient documentation so maintenance and future changes are facilitated.